



AR
Ifw

TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>		Application No.	10/087,576
		Filing Date	March 1, 2002
		First Named Inventor	Richard P. Mangold
		Art Unit	2135
		Examiner Name	Beemnet W. Dada
Total Number of Pages in This Submission	47	Attorney Docket Number	42390P12445

ENCLOSURES <i>(check all that apply)</i>		
<input checked="" type="checkbox"/> Fee Transmittal Form <input checked="" type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment / Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> PTO/SB/08 <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/Incomplete Application <input type="checkbox"/> Basic Filing Fee <input type="checkbox"/> Declaration/POA <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation, Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) <input type="checkbox"/> Landscape Table on CD	<input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to TC <i>(Appeal Notice, Brief, Reply Brief)</i> <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) <i>(please identify below):</i> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Return Postcard Check for \$500.00</div>
Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	Jose R. Mata, Reg. No. 56,978 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	October 18, 2006

CERTIFICATE OF MAILING/TRANSMISSION			
I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.			
Typed or printed name	Gayle Bekish		
Signature		Date	October 18, 2006



FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT (\$)
500.00

Complete if Known

Application Number	10/087,576
Filing Date	March 1, 2002
First Named Inventor	Richard P. Mangold
Examiner Name	Beemnet W. Dada
Art Unit	2135
Attorney Docket No.	42390P12445

METHOD OF PAYMENT (check all that apply)

☒ Check ☐ Credit card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee
☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20. ☒ Credit any overpayments

FEE CALCULATION

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500.00
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) _____

SUBTOTAL (2) (\$)
500.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Jose B. Mata	Registration No. (Attorney/Agent)	56,978	Telephone	(310) 207-3800
Signature		Date	10/18/06		



Attorney's Docket No. 42P12445

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application for:

Richard Mangold, et al.

Serial No. 10/087,576

Filed: March 1, 2002

For: Transparently Embedding Non-Compliant
Data In a Data Stream

Examiner: Beemnet W. Dada

Art Unit: 2135

Assistant Commissioner for Patents
Board of Patent Appeals and Interferences
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

In support of their appeal, Applicants submit the following Appellate Brief for consideration by the Board of Patent Appeals and Interferences ("Board"). Please charge any additional amounts due or credit any overpayment to Deposit Account No. 02-2666.

10/24/2006 AWONDAF1 00000017 10087576

01 FC:1402

500.00 OP

TABLE OF CONTENTS

I.	Real Party in Interest.....	4
II.	Related Appeals and Interferences.....	4
III.	Status of Claims	4
IV.	Status of Amendments	4
V.	Summary of Claimed Subject Matter	5
VI.	Grounds of Rejection	9
VII.	Argument	9
A.	Overview of Cited Reference: U.S. Patent No. 5,805,705 issued to Gray <i>et al.</i> (“Gray”)	9
B.	Claims Rejected Under 35 U.S.C. § 102(b).....	10
1.	Regarding Claims 1 and 2.....	11
a)	<i>Gray does not Describe Replacing Non-Compliant Data</i>	11
b)	<i>Gray does not Describe Placing Non-Compliant Data</i>	15
c)	<i>Gray does not Describe a Data Stream that is Decodable</i>	15
2.	Regarding Claim 3.....	17
3.	Regarding Claim 4	18
4.	Regarding Claim 5	19
5.	Regarding Claim 6	20
6.	Regarding Claim 7	21
7.	Regarding Claim 8	22
8.	Regarding Claim 9	23
9.	Regarding Claim 10	24
10.	Regarding Claim 11	25

11. Regarding Claim 12	26
12. Regarding Claim 13	27
13. Regarding Claim 14	27
14. Regarding Claim 15	28
15. Regarding Claim 16	29
16. Regarding Claim 17	29
17. Regarding Claim 18	30
18. Regarding Claim 19	31
C. Claims Rejected Under 35 U.S.C. §103(a)	31
1. Regarding Claims 20, 24, 25	31
2. Regarding Claim 21	33
3. Regarding Claim 22	34
4. Regarding Claim 23	34
VIII. Claims Appendix	37
IX. Evidence Appendix	43
X. Related Proceedings	44

I. REAL PARTY IN INTEREST

The inventors, Richard P. Mangold, Keith L. Shippy, and Ajit P. Joshi assigned their rights in that which is disclosed in the subject application to Intel Corporation of Santa Clara, California through assignments that were recorded March 1, 2002 (Reel/Frame: 012668/0711). Intel Corporation is therefore the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-25 are pending in this application. All claims stand rejected. Applicant seeks individual review of each of claims 1-25, based on separate arguments presented in support of independent claims 1, 5, 8, 11, 14, 20 and dependent claims 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18, 19, 21, 22, and 23.

IV. STATUS OF AMENDMENTS

Applicants submitted proposed amendments to claims 8 and 20-25 in an Amendment and Response to Final Office Action that was filed July 6, 2002. The Office entered those amendments in an Advisory Action mailed July 20, 2006. Thus, all proposed amendments in the Amendment and Response to Final Office Action have been entered. No other amendments were submitted after the Final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the invention relate to transparently embedding non-compliant data in a data stream (p. 2, lines 8-9). Non-compliant data is data which does not strictly comply with a standard, such as one of the Moving Pictures Experts Group (MPEG) standards (p. 4, lines 14-15; MPEG identified at p. 1, lines 11-13). The non-compliant data is, for example, navigation information or any other kind of information not strictly allowed by the standard (p. 4, lines 15-16). Key information is one example of non-compliant data (p. 4, lines 7-8 – discussing replacement of key information with compliant data). Key information is any information useful to any cryptographic algorithm, such as one or more random numbers (p. 2, line 31 – p. 3, line 1). Embedding non-compliant data, such as key information, in a data stream would normally cause an MPEG standard-compliant decoder to fail (p. 1, lines 13-15). In some embodiments, a data stream is decodable by a compliant decoder, after non-compliant data is replaced with compliant data (p. 5, lines 5-7).

Independent claim 1 is a method comprising parsing a data stream to find a predefined synchronization point within the data stream (Fig., 5, feature 502; p. 5, lines 3-4; p. 5, line 7, note that the text recites that, “An example of a synchronization point is a header.”), placing non-compliant data near the synchronization point in the data stream (Fig. 5, feature 504; p5, lines 4-5), wherein the data stream is decodable by a compliant decoder (Fig. 5, feature 508; p. 5 lines 5-6), after the non-compliant data is replaced by compliant data (Fig. 5, features 506; p. 5 lines 6-7).

Dependent claims 3 and 4 are argued separately. Because claim 4 depends from claim 3, which depends from claim 2, all three are summarized. Dependent claim 2 modifies the method of claim 1 to include encrypting a portion of the data stream; and transmitting the portion of the

data stream (p. 5, lines 8-9). Dependent claim 3 modifies the method of claim 2 to include decrypting the portion of the data stream (p. 5, line 10). Dependent claim 4 refines the method of claim 3 so that the non-compliant data is key information that is used in encrypting and decrypting (p. 5, lines 11-12).

Independent claim 5 is a method comprising receiving a portion of a data stream (Fig. 4, feature 402; p. 4, lines 16-17), parsing the portion of the data stream to find a synchronization point within the data stream (Fig. 4, feature 404; p. 4, lines 17-18), retrieving non-compliant data near the synchronization point (Fig. 4, feature 406; p. 4, lines 19-20), replacing non-compliant data in the data stream (p. 4, lines 22-23), and decrypting the portion of the data stream (Fig. 4, feature 408, p. 4, line 20).

Dependent claim 6 modifies the method of claim 5 so that the non-compliant data is key information that is used in decrypting (p. 4, line 21).

Dependent claim 7 modifies the method of claim 5 to include replacing the non-compliant data near the synchronization point with compliant data and decoding the portion of the data stream (p. 4 lines 22-24).

Independent claim 8 is drawn to a system (Fig. 1, feature 100; p. 2 lines 18-19) comprising an authoring device (Fig. 1, feature 102; p. 2 lines 18-19) to use key information to encrypt a portion of a data stream (p. 2, lines 29-30), and a consumption device (Fig. 1, feature 104; p. 2 lines 18-19) in communication with the authoring device (p. 3, lines 23-27, text describes content “transmitted” from “authoring device 102” to “the consumption device 104”), the consumption device to use the key information to decrypt the portion of the data stream (p. 2, lines 30-31) and to replace the key information with compliant data (p. 3, lines 27-31 – “key

information replaced with stuffing bytes”; p. 7, lines 3-4 – text describing “stuffing bytes, which are predefined in the MPEG standards”).

Dependent claim 9 refines the system of claim 8 to include a decoding device in communication with the consumption device (Fig. 1, feature 106; p. 3, lines 15-17) to decode the portion of the data stream (p. 3, lines 17-18).

Dependent claim 10 refines the system of claim 8, reciting that the consumption device is configured to retrieve the key information from the portion of the data stream (p. 3, lines 21-23).

Independent claim 11 is drawn to a system (Fig. 2, feature 200; p. 4, lines 1-3) comprising an authoring device (Fig. 2, feature 202; p. 4, lines 1-3) to create a data stream (p. 4, lines 3-4), an encryption tool (Fig. 2, feature 204; p. 4, lines 1-3) to embed key information near each synchronization point in the data stream and to encrypt a portion of the data stream associated with each synchronization point (p. 4, lines 4-6), and a consumption device (Fig. 2, feature 206; p. 4, lines 1-3) to retrieve key information near each synchronization point in the data stream and to replace the key information with compliant data (p. 4, lines 6-8) and to use the key information to decrypt the data stream (p. 3, lines 27-29; p. 4 line 8).

Dependent claim 12 refines the system of claim 11 to include a decoding device to decode the data stream (Fig. 2, feature 208; p. 4, lines 8-9).

Dependent claim 13 refines the system of claim 11 to include a decryption tool to use the key information to decrypt the portion (Fig. 3, feature 302; p. 4, lines 9-11).

Independent claim 14 is drawn to a machine-accessible medium (p. 6, lines 4-5) having associated content capable of directing the machine to perform a method comprising a machine-accessible medium having associated content capable of directing the machine to perform a method comprising parsing a first data stream to find a packetized element stream (PES) header

(Fig. 6, Feature 602; p. 6, lines 5-6), the PES header associated with at least some payload data (p. 6, lines 6-7), copying the first data stream to a second data stream (Fig. 6, Feature 604; p. 6, line 7), and selectively inserting compliant data into the second data stream after the PES header, to hold key information associated with the PES header (Fig. 6, Feature 606; p. 6, lines 8-9).

Dependent claim 15 modifies the machine-accessible medium of claim 14 so that the method includes storing the first data stream and storing the second data stream (p. 6, lines 10-11).

Dependent claim 16 modifies the machine-accessible medium of claim 14 so that the method includes parsing the second data stream to find each PES header (p. 6, lines 11-12), embedding key information into each portion of the second data stream after each PES header (p. 6, lines 12-13), and encrypting each portion of the second data stream (p. 6, lines 13-14).

Dependent claim 17 modifies the machine-accessible medium of claim 16 so that the method includes transmitting each portion of the second data stream (p. 6, lines 14-15).

Dependent claim 18 modifies the machine-accessible medium of claim 16 so that the method includes retrieving key information from a portion of the second data stream (p. 6, lines 16-17), decrypting the portion of the second data stream with the key information (p. 6, lines 17-18), and replacing the key information with compliant data in the portion of the second data stream (p. 6, lines 18-19).

Dependent claim 19 modifies the machine-accessible medium of claim 18 so that the method includes decoding the portion (p. 6, lines 19-20).

Independent claim 20 is a method comprising transmitting a data structure to a consumption device, the data structure including a header, key information separate from and associated with the header for use in decryption, and a payload associated with the header, the

payload capable of being encrypted using the key information (Fig. 8, feature 800; p. 7, lines 23-26). Claims 20, 24 and 25 are argued jointly.

Dependent claim 21 modifies the method of claim 20 to recite that compliant data replaces the key information associated with the header, before decryption (Fig. 8, feature 802; page 7 lines 28-29).

Dependent claim 22 modifies the method of claim 20 to recite that the header, compliant data, and decrypted payload are capable of being decoded by a compliant decoder (Fig. 8, feature 804; page 7 lines 29-31).

Dependent claim 23 modifies the method of claim 20 to recite that the key information in the header replaces compliant data, after encryption (page 7 lines 26-28).

VI. GROUND OF REJECTION

Claims 1-19 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,805,705 issued to Gray *et al.* (“Gray”).

Claims 20-25 stand rejected under 35 U.S.C. § 103(a) as unpatentable over *Gray*. There is no secondary reference.

VII. ARGUMENT

A. Overview of Cited Reference: U.S. Patent No. 5,805,705 issued to Gray *et al.* (“Gray”)

Gray describes a simple communication technique that uses a bit value as a flag. Specifically, *Gray* describes a data communication network in which encryption/decryption keys are periodically exchanged between connected source and destination nodes (Abstract). A

destination node not only needs to know the value of a new key, but it must know when to start using the new key. *Id.* For this purpose, destination nodes examine a single dedicated bit in each packet header – a “key synchronization bit” (KSB). *Id.* As long as the bit value in arriving packets remains unchanged from one received packet to the next, a destination node continues to use the current decryption key to decrypt data. *Id.* When a packet arrives with a different bit value, the destination node begins using a previously-received, new decryption key. *Id.* The KSB acts essentially as a simple flag.

Although *Gray* describes network-level packets, such as Asynchronous Transfer Mode (ATM) packets (*Gray*, e.g., col. 3, lines 45-51), *Gray* does not describe application-level packets or data streams that comply with a standard, such as one of the MPEG standards. Thus, *Gray* does not discuss ways of distinguishing between data streams that comply or do not comply with such application-level standards.

Gray has little in common with the claimed invention in this case, other than that they both involve encryption/decryption on networks. *Gray* does not describe transparently embedding non-compliant data – such as key information – in a data stream. *Gray* certainly does not describe replacing non-compliant data in a data stream with compliant data to render the data stream decodable by a compliant decoder. Indeed, *Gray* does not describe encoding/decoding (as contrasted with encrypting/decrypting) of data streams.

B. Claims Rejected Under 35 U.S.C. § 102(b)

Claims 1-19 were rejected as anticipated by *Gray*. "A claim is anticipated only **if each and every element as set forth in the claim** is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131 quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (emphasis added).

Further, "[t]he **identical invention** must be shown in **as complete detail as is contained in the ... claim.**" *Id.*, quoting, *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added). For at least the reasons discussed below, the following claims are not anticipated by *Gray*.

1. Regarding Claims 1 and 2

Claim 1 recites:

1. A method, comprising:

parsing a data stream to find a predefined synchronization point within the data stream; and

placing non-compliant data near the synchronization point in the data stream; wherein the data stream is decodable by a compliant decoder, after the non-compliant data is replaced with compliant data (Emphasis added).

At least the emphasized portions of claim 1 recite limitations that are not taught by *Gray*.

a. *Gray* does not Describe Replacing Non-Compliant Data with Compliant Data.

Claim 1 recites replacing the non-compliant data with compliant data so that the data stream is decodable by a compliant decoder. *Gray* does not teach replacing the non-compliant data with compliant data. The Office action relies on col. 5, lines 23-35 as teaching the above limitation (Office Action, p. 4, ¶ 15). The Office summarizes this portion of *Gray* as describing "decrypting data with the key, which is changed when the synchronization bit changes" *Id.* It is unclear from this passage whether the Office regards the key or the KSB as corresponding to the replaced non-compliant data. However, the following analysis demonstrates that neither corresponds to the replaced non-compliant data of claim 1.

i) The KSB is not Non-Compliant Data that is Replaced with Compliant Data.

In the following portion of the Office Action, the Office argues that *Gray*'s KSB is non-compliant data that is replaced:

Examiner would point out that the terms “non-compliant data” and “compliant data” are not defined in the specification. It is interpreted by the examiner, that changing the synchronization bit from a ‘0’ to a ‘1’ or vice-versa, as key information so that the correct encryption/decryption keys can be used meets the limitation where a non-compliant data is replaced with compliant data . . . (Office Action, p. 2, ¶ 4).

The Office is incorrect for at least two reasons. First, the KSB bit value is not replaced. When the bit value of the KSB is changed from one packet to the next, no data is replaced. No data within a packet is changed. The destination nodes monitor the change in the KSB between packets – not a change of the KSB within a single packet.

Monitoring the changing of the value of the KSB between packets is not equivalent to the replacement of non-compliant data with compliant data as set forth in claim 1. The term “replace” means “to take or fill the place of.” See the American Heritage Dictionary of English Language 4th edition, Houghton Mifflin Co. (2000). Thus, according to claim 1, compliant data is put in the place of non-compliant data. This is not disclosed by *Gray*. The section of *Gray* cited by the Office discloses that a synchronization bit, which may be either a value of 0 or 1, may change from one packet to the next over time. It does not teach that any given synchronization bit value is replaced at the same position in the same packet by another value. See *Gray* col. 4, lines 52-56 which states that “a change in the binary value stored in KSB position 56 from one data packet to the next is a signal to a destination node that a new decryption key (previously sent to and stored by the node) is to be activated” (emphasis added). See also col. 5, lines 13-22. Thus, the sections of *Gray* that the Office relies on to teach the replacing of non-compliant data with compliant data, in fact, teach only the monitoring of the changing of a value from one data

packet to the next as an indicator that a decryption key should be changed. This does not teach that any data is put in the place of other data and thus it cannot be said that *Gray* teaches replacing any data.

In an Advisory Action of July 20, 2006 (“Advisory Action”) the Office maintains its rejection and argues:

applicant argued that *Gray* fails to teach replacing non-compliant data with compliant data. Examiner disagrees. Examiner would point out that *Gray* teaches replacing/changing the KSB value to a 1 or a 0 Therefore, *Gray* teaches the claim limitations, the data stream is decodable by a compliant decoder after the non-compliant data is replaced with compliant data (i.e., decrypting data with the key, which is changed with the synchronization bit changes) . . . (Advisory Action, continuation sheet).

But the above does not explain how having the KSB bit value be a ‘0’ in a first packet and a ‘1’ in a second packet teaches the replacing of data. After the KSB is set to ‘1’ in the second packet, the KSB bit value in the first packet remains ‘0.’ No data is replaced. Thus, the *Gray* KSB is not data that is replaced as recited by claim 1. Therefore *Gray* does not teach this replacement limitation of claim 1 and does not anticipate claim 1.

The Office’s position that the KSB is replaced non-compliant data is incorrect for a second reason. The KSB is not non-compliant data. In the above-quoted passage, the Office ignores the plain meaning of the terms “non-compliant data” and “compliant data.” The word “compliant” is a form of “comply” which means “to conform, submit, or adapt” – for example, “the devices comply with industry standards.” Webster’s Online Dictionary, www.webster.com (2006). Non-compliant data therefore is data that does not comply with a standard, such as one of the MPEG standards (*See, e.g.*, Specification, p. 4, lines 14-15).

Gray does not describe the KSB as non-compliant with any standard. The Office Action at p. 4, ¶15 cites col. 4, lines 46-58 of *Gray* as describing “placing non-compliant data . . . in the data stream.” This portion of *Gray* describes defining a single bit position of a header byte as the KSB. It does not, however, describe the KSB as non-compliant with any standard. Again at p. 4, ¶ 15, the Office Action cites col. 5, lines 23-35 of *Gray* as describing “the data stream decodable by a compliant decoder, after the non-compliant data is replaced with compliant data.” This portion of *Gray* describes using the KSB to signal a destination node to activate and use a new key for decryption. But there is no discussion of the KSB being non-compliant with any standard. Thus, *Gray* does not describe the KSB as being non-complaint with any standard. Therefore, the *Gray* cannot describe the KSB as being replaced non-compliant data.

ii) The Keys are not Non-Compliant Data

The Office would also be incorrect in regarding the current and new decryption keys as the non-compliant and compliant data of claim 1. Regarding keys, *Gray* describes that when the KSB bit value changes, “the new key is retrieved from storage and activated to decrypt the packet payload.” (*Gray*, col. 5, lines 33-34). But using a new key and discontinuing use of the current key does not meet the above limitation of claim 1 for several reasons.

The “current decryption key” and the “new key” are not described as being placed in a data stream. But claim 1 recites “placing non-compliant data . . . in the data stream.” The compliant data replaces the non-compliant data in the data stream. Therefore, the current and new keys cannot reasonably be construed, respectively, as “non-compliant data” and “compliant data” as those terms are used in claim 1.

Indeed, *Gray* does not describe how the keys are moved or stored, stating, “[t]he specific key exchange protocol employed is not critical to the present invention. It only matters that the

new key is sent to the destination node” (*Gray*, col. 5, lines 3-5). Because the current and new keys are not described as being placed in a data stream, they do not correspond to the compliant and non-compliant data of claim 1.

In addition, neither the “current decryption key” nor the “new key” is described by *Gray* as being non-compliant with any standard. Thus, neither of these keys are non-compliant data. Therefore, *Gray* does not describe the above limitation regarding replacing non-compliant data with compliant data. *Gray* does not anticipate claim 1.

b. *Gray* does not Describe Placing Non-Compliant Data in a Data Stream.

Claim 1 also recites “placing non-compliant data near the synchronization point in the data stream” (emphasis added). The Office Action finds that this placing limitation is described in col. 4, lines 46-58 of *Gray*, which describes defining a bit in a header as the KSB (Office Action, p. 4, ¶ 15). Thus, by citing this portion of *Gray* the Office is apparently arguing that the KSB is the non-compliant data that is placed in the data stream.

However, as discussed above, *Gray* does not describe the KSB as being non-compliant with any standard. Therefore, the KSB cannot be non-compliant data as recited in claim 1. Because the KSB is not non-compliant data, defining a bit in a header as the KSB is not placing non-compliant data in a data stream. *Gray* thus fails to teach at least this limitation of claim 1 and therefore does not anticipate claim 1.

c. *Gray* does not Describe a Data Stream that is Decodable by a Compliant Decoder.

Claim 1 recites that once the non-compliant data is replaced with compliant data, “the data stream is decodable by a compliant decoder. In finding that *Gray* describes this limitation of claim 1, the Office uses decrypt and decode interchangeably: “Therefore, *Gray* teaches the

claim limitations, the data stream is **decodable** by a compliant decoder . . . (i.e., **decrypting data** with the key . . .)”(Advisory Action, Continuation Sheet, citing *Gray* col. 5, lines 23-35) (emphasis added).

However, decoding and decrypting are often used to refer to different actions. For example, in the attached article, “An Empirical Study of Secure MPEG Video Transmissions,” Iskender Agi and Ki Gong, SRI International Computer Science Laboratory, IEEE (1996) (Available for download: <http://citeseer.ist.psu.edu/3765.html>), the authors recognize that encryption and encoding are not necessarily the same:

No provision for **encryption** was included for MPEG transmissions. The very nature of MPEG **encoding** – the encoding of inherently spatially and temporally correlated video – makes encryption difficult [citation omitted] . . . MPEG uses an asymmetric coding model where **encoding** requires substantial more computational power than **decoding**. Adding security to MPEG transmission usually involves encrypting parts or the whole MPEG bit stream. It has been recognized that commonly available software and hardware encryption mechanisms often cannot encrypt entire MPEG streams without severely degrading performance and quality of service.

Id. p. 1.

Thus, those skilled in the art may use encryption/decryption to cryptographic actions while using encode/decode to refer to compression/decompression – as in the case of the above MPEG article.

Applicants have similarly used encryption/decryption as distinct from encoding/decoding. Applicants are entitled to act as their own lexicographers to refer to encryption/decryption and encoding/decoding as different and distinct actions. MPEP § 2111.01(III). For example, Fig 3 of the Specification depicts decryption tool 302 and decoding device 208. The text of the Specification also refers to decrypting and decoding as distinct, e.g., “**The decoder** receives the packetized element stream (PES) header, the stuffing bytes, and the

decrypted PES payload and then decodes as usual” (Specification, p. 3, lines 31-32). The Specification refers to decoding as interpreting an encoded data stream. For example, in discussing a decoding device 106 of Fig. 1, the Specification states, “The decoding device 106 is any device capable of interpreting the data stream, such as an MPEG-compliant decoder” (p. 3, lines 18-19) (emphasis added).

The above distinction between encryption/decryption and encoding/decoding is carried forward in the claims. Claim 1 recites “wherein the data stream is decodable by a compliant decoder.” In contrast, dependent claim 3 recites that the method of claim 1 further comprises “decrypting the portion of the data stream.” Similarly, independent claim 5 recites “decrypting the portion of the data stream” and dependent claim 7 modifies the method of claim 5 to further comprise “. . . decoding the portion of the data stream.” Thus, as used in the claims, decoding and decrypting are distinct.

However, *Gray* describes only encrypting/decrypting and not encoding/decoding. As discussed above, the Office – in the Advisory Action Continuation Sheet – finds that “the data stream decodable by a compliant decoder” is described at col. 5, lines 23-35 of *Gray*. However, this portion of *Gray* describes only decrypting, not decoding. Because *Gray* describes only decrypting and not decoding, it does not describe at least the above limitation of claim 1. Therefore, *Gray* does not anticipate claim 1.

For at least the above reasons, claim 1 is separately patentable and it is requested that the Board overturn the rejection of claim 1. Claim 2 is patentable because it depends from 1 and it is therefore requested the Board overturn the rejection of claim 2.

2. Regarding Claim 3

Claim 2 modifies the method of claim 1 to recite, “encrypting a portion of the data stream; and transmitting the portion of the data stream. Claim 3 modifies the method of claim 2 to recite, “decrypting the portion of the data stream.”

Applicants assert that, as used in their specification and claims, decoding is distinct from decrypting. If the Board finds that discussion of decryption in *Gray* reads on the decodable data stream limitation of claim 1, then the Board should also find that *Gray* does not read on the decrypting limitation of claim 3.

For at least the above reasons, claim 3 is separately patentable and it is requested that the Board overturn the rejection of claim 3.

3. Regarding Claim 4

Claim 2 modifies the method of claim 1 to recite, “encrypting a portion of the data stream; and transmitting the portion of the data stream. Claim 3 modifies the method of claim 2 to recite, “decrypting the portion of the data stream. Finally, claim 4 modifies the method of claim 3 to recite, “wherein the **non-compliant data is key information that is used in encrypting and decrypting**” (emphasis added). *Gray* does not teach this limitation of claim 4 and therefore does not anticipate claim 4.

Regarding claim 4, the Office cites col. 4, lines 49-57 and argues that claim 4 is met by the “KSB value associated with current or next key value” that is used for encrypting and decrypting. But the Office’s argument depends upon the KSB being the claimed non-compliant data. The key information is recited as non-compliant data. Applicants rely on the arguments made in support of claim 1 that the KSB is not non-compliant data. Therefore, whether the KSB is used for encrypting and decrypting is irrelevant. *Gray* does not teach using non-compliant data for encrypting and decrypting a data stream.

Furthermore, the KSB is not key information because it is not actually used in performing encrypting or decrypting. The KSB is simply a signal to start using the new key. There is no interaction between the key and the KSB the way there would be between, for example, a key and a random number. Nor is the KSB encrypted using the key. The KSB operates before decryption, but is not used in the decryption.

In addition, the KSB is not used by the source nodes of *Gray* to perform encryption. The KSB is read by the destination nodes as a flag to switch to a new key for decryption. Claim 4 requires that the non-compliant data – the key information – be used in both encrypting and decrypting.

For at least these reasons, Applicants submit that claim 4 is not anticipated by *Gray*. For at least the above reasons, claim 4 is separately patentable and it is requested that the Board overturn the rejection of claim 4.

4. Regarding Claim 5

Independent claim 5 recites:

5. A method, comprising:
- receiving a portion of a data stream;
 - parsing the portion of the data stream to find a synchronization point within the data stream;
 - retrieving non-compliant data** near the synchronization point;
 - replacing** non-compliant data in the data stream; and
 - decrypting the portion of the data stream.

(Emphasis added).

The emphasized portions of claim 1 recite at least several limitations that are not taught by *Gray*.

The first emphasized portion of claim 5 recites “retrieving non-compliant data near the synchronization point.” An example of a synchronization point is a packetized element stream

header (Specification, p. 4, lines 18-19). This limitation of claim 5 would not be met because the KSB is not described by *Gray* as non-compliant data. Claim 5 recites that non-compliant data be retrieved. Applicants rely on their argument regarding claim 1 that the KSB is not described by *Gray* as non-compliant data. Thus, *Gray* does not describe this limitation of claim 5.

The second emphasized portion of claim 5 recites “replacing non-compliant data in the data stream.” Applicants note that the Office interprets this limitation as “replacing synchronization bit.” (Office Action, p.5, ¶ 16). In support of its rejection, the Office first cites col. 4, lines 46-68 and col. 5, lines 7-35 of *Gray*. These passages describe defining a bit in a header as the KSB and further describe using the KSB as a signal to the destination node to begin using a new key for decryption. Nothing therein describes the KSB as non-compliant with a standard or describes the KSB as being replaced in a data stream. Applicants rely upon their arguments on behalf of claim 1 that *Gray* does not describe the KSB as non-compliant data and that *Gray* does not describe replacing non-compliant data in a data stream.

For at least the above reasons, claim 5 is separately patentable and it is requested that the Board overturn the rejection of claim 5.

5. Regarding Claim 6

Dependent claim 6 modifies the method of claim 5 to recite that the non-compliant data of claim 5 is “key information that is used in decrypting.” Putting claim 6 in context, it is recalled that claim 5 recites retrieving and replacing the non-compliant data near a synchronization point in a portion of a data stream. Claim 5 further recites decrypting the portion of the data stream. The limitation of claim 6 specifies that the above non-compliant data

is “key information” that is used in the above decrypting of the portion of the data stream. *Gray* does not teach the above limitation of claim 6 and therefore does not anticipate claim 6.

In rejecting claim 6, the Office argues that the key information of claim 6 is the KSB “associated with current or next key value” that is used in encrypting and decrypting. (Office Action, p. 6, ¶ 21). The Office relies on col. 4, lines 49-57 of *Gray*. (*Id.*). The cited portion of *Gray* merely describes that once the value of the KSB is changed, the destination node activates a new key for decryption.

But the Office overlooks that the key information used in the decrypting must be the non-compliant data that is retrieved and replaced in claim 5. Even if one assumes for purposes of argument that the KSB is non-compliant data, there is nothing in this cited portion of *Gray* that describes the KSB as being retrieved or replaced from a portion of a data stream and then being used to decrypt that portion of the data stream. Thus, the cited portion of *Gray* does not describe the above limitation of claim 6.

For at least the above reasons, claim 6 is separately patentable and it is requested that the Board overturn the rejection of claim 6.

6. Regarding Claim 7

Dependent claim 7 modifies the method of claim 5 to further comprise, “replacing the non-compliant data near the synchronization point with compliant data; and **decoding** the portion of the data stream.” (Emphasis added).

In rejecting claim 7, the Office cites col. 5, lines 23-34 of *Gray*. (Office Action, p. 6, ¶ 7). But there is nothing in the cited passage that appears to be either a synchronization point or non-compliant data that is near that synchronization point. The passage simply describes receiving a new key and then beginning to use it when the KSB value changes.

If one assumes the Office intends the new key to be the non-compliant data that is replaced, then – as argued regarding claim 1 – there is nothing to support the position that a key is non-compliant data.

Applicants also rely on their argument in support of claim 1 that the KSB is not non-compliant data and that *Gray* does not describe replacing non-compliant data in a data stream.

Regarding the “decoding the portion of the data stream” limitation, Applicants rely on their argument in support of claim 1 that *Gray* does not teach a decodable data stream or decoding.

Thus, *Gray* does not teach the limitations of claim 7. For at least the above reasons, claim 7 is separately patentable and it is requested that the Board overturn the rejection of claim 7.

7. Regarding Claim 8

Independent claim 8 recites:

8. A system, comprising:
an authoring device to use key information to encrypt a portion of a data stream; and
a consumption device in communication with the authoring device, the consumption device **to use the key information to decrypt the portion of the data stream and to replace the key information with compliant data.**

(Emphasis added).

Thus, the emphasized portion of claim 8 recites a consumption device using key information to decrypt a portion of a data stream and replacing the key information with compliant data.

In rejecting claim 8, the Office cites col. 2, lines 50-67 of *Gray*. This cited passage describes providing a new key to a destination node and using the KSB value to communicate to the destination node when it is time to start using the new key. But the passage does not describe using key information to decrypt a portion of a data stream and replacing the key with compliant data. Further, there is nothing in the cited passage describing any data as complying with any

standard. Thus, the passage does not describe any compliant data that replaces the non-compliant data.

If the Office is arguing that the KSB corresponds to the key information of claim 8, then the Office must show that the KSB is non-compliant data and that it is replaced by compliant data. Key information is an example of non-compliant data – “In another embodiment, the non-compliant data is key information that is used in decrypting.” (Spec., p. 4, lines 20-21). Applicants rely on their arguments in regard to claim 1 that *Gray* describes neither non-compliant data nor replacing non-compliant data. This includes Applicants arguments that the KSB is not non-compliant data and that changing the bit value of the KSB is not the replacement of non-compliant data.

Applicants also rely on their arguments in support of claim 4 that, the KSB is not key information because it is not actually used in performing encryption or decryption.

For the above reasons, the KSB in the cited passage cannot correspond to the key information of claim 8. For at least the above reasons, claim 8 is separately patentable and it is requested that the Board overturn the rejection of claim 8.

8. Regarding Claim 9

Dependent claim 9 refines the system of claim 8 by reciting that the system further comprises, “a decoding device in communication with the consumption device to decode the portion of the data stream.”

In rejecting claim 9, the Office cites col. 5, lines 23-34 of *Gray*. This cited passage merely describes decryption – not decoding and not a decoding device. Applicants argued regarding claim 1 that *Gray* does not teach a decodable data stream or decoding. That argument will not be repeated, but is fully applicable to claim 9.

Further, claim 9 includes the limitations of claim 8. Thus, the Office must show that *Gray* describes a decoder to decode a portion of a data stream that – as recited in claim 8 from which claim 9 depends – has been decrypted by a consumption device that used key information to perform the decryption and that replaced the key information with compliant data. The Office cannot show the above because *Gray* does not teach the above limitations.

For at least the above reasons, claim 9 is separately patentable and it is requested that the Board overturn the rejection of claim 9.

9. Regarding Claim 10.

Dependent claim 10 refines the system of claim 8 by reciting that, “the consumption device is configured to retrieve the key information from the portion of the data stream.”

In rejection claim 10, the Office cites only col. 5, lines 23-34 of *Gray*, which the Office describes as teaching, “replacing the non-compliant data near the synchronization point with compliant data, and decoding the portion of the data stream” (Office Action, p. 6, ¶ 22). Thus, the Office cites a passage to teach a limitation that is not recited by claim 10. The Office does not cite any other portion of *Gray* as teaching the limitation of claim 10. Applicants assert that no portion of *Gray* describes what is recited in claim 10.

Applicants rely on their arguments in support of claim 8 that key information is non-compliant data and that the KSB is not key information. Applicants also rely on their arguments in support of claim 5 that *Gray* does not describe retrieving non-compliant data. Applicants further rely on their arguments in support of claim 1 that *Gray* does not describe the KSB as non-compliant data.

For at least the above reasons, claim 10 is separately patentable and it is requested that the Board overturn the rejection of claim 10.

10. Regarding Claim 11.

Independent claim 11 recites:

11. A system, comprising:

an authoring device to create a data stream;

an encryption tool to embed key information near each synchronization point in the data stream and to encrypt a portion of the data stream associated with each synchronization point; and

a consumption device to retrieve key information near each synchronization point in the data stream and to replace the key information with compliant data and to use the key information to decrypt the data stream.

(Emphasis added).

The first emphasized portion of claim 11 recites an encryption tool that both embeds key information near each synchronization point and encrypts a portion of a data stream associated with each synchronization point. *Gray* does not describe embedding and encrypting near synchronization points in a data stream. In rejecting this portion of claim 11, the Office cites col. 4, lines 49-67 of *Gray*. (Office Action, p. 5, ¶ 18).

The above-cited passage describes defining a bit in a header as the KSB. It further describes, from a source node's perspective, using the KSB as a signal to a destination node to activate a new decryption key. Although the passage does describe "data packets" (col. 4, line 62), it does not describe synchronization points in a data stream. The passage certainly does not describe embedding key information near each synchronization point in a data stream. Nor does the passage describe encrypting a portion of a data stream associated with synchronization point in a data stream. Thus, *Gray* fails to teach at least this limitation of claim 11.

The second emphasized portions of claim 11 recite a consumption device. The consumption device retrieves key information near each synchronization point in a data stream. In rejecting this limitation of claim 11, the Office cites col. 5, lines 23-34 of *Gray*. (Office

Action, p. 6, ¶ 18). This portion of *Gray* merely describes a method of using the KSB to signal a destination node when to activate and use a new key. Although this passage does describe retrieving a new key for activation, there is no description of the key being retrieved from a data stream. As discussed above regarding claim 1, *Gray* does not describe how keys are exchanged between source and destination nodes.

To the extent the Office is once again relying on the KSB as the key information, Applicants rely on their argument in support of claim 8 that key information is non-compliant data and that the KSB is not key information. Further, there is no description of the KSB being retrieved. Thus, *Gray* fails to teach at least this limitation of claim 11.

Claim 11 also recites that the consumption device replaces key information with compliant data and uses the key information to decrypt a data stream. With respect to this limitation, Applicants rely on their arguments made supporting the consumption device limitation of claim 8.

Regarding those portions of claim 11 reciting the embedding and retrieving of key information, Applicants rely on their argument in support of claim 8 that key information is non-compliant data and that *Gray* does not describe the KSB as key information. Applicants also rely on their arguments in regard to claim 1 that *Gray* does not describe the KSB as non-compliant data.

For at least the above reasons, claim 11 is separately patentable and it is requested that the Board overturn the rejection of claim 11.

11. Regarding Claim 12.

Dependent claim 12 refines the system of claim 11 by reciting, “a decoding device to decode the data stream.” Applicants rely upon their arguments made in support of claims 3 and

9 the *Gray* does not describe decodable data streams or decoding For at least the above reasons, claim 12 is separately patentable and it is requested that the Board overturn the rejection of claim 12.

12. Regarding Claim 13.

Dependent claim 13 refines the system of claim 11 by reciting “a decryption tool to use the key information to decrypt the portion.” Applicants rely on their argument in support of claim 8 that key information is a type of non-compliant data and that the KSB is not key information. Applicants also rely on their arguments in support of claim 1 that *Gray* does not describe the KSB as non-compliant data. For at least the above reasons, claim 13 is separately patentable and it is requested that the Board overturn the rejection of claim 13.

13. Regarding Claim 14.

Independent claim 14 recites:

14. A machine-accessible medium having associated content capable of directing the machine to perform a method, the method comprising:
parsing a first data stream to find a packetized elementary stream (PES) header, the PES header associated with at least some payload data;
copying the first data stream to a second data stream; and
selectively **inserting compliant data into the second data stream after the PES header, to hold key information associated with the PES header.**
(Emphasis added).

In rejecting claim 14, the Office relied upon the same portions of *Gray* as it did to reject claim 1. (Office Action, p. 4, ¶ 15) (citing col. 5, lines 23-29; col. 4, lines 46-58; col. 5, lines 23-35 of *Gray*). Yet the claims are quite different.

The Office does not specifically cite any portion of *Gray* as describing the limitation of copying a first data stream to a second data stream. Reviewing the portions of *Gray* that the Office cited in rejecting claim 1, none of those portions describes the above limitation. Nor does any other portion of *Gray* describe the above limitation. Therefore, *Gray* fails to teach at least this limitation of claim 14 and does not anticipate claim 14.

Claim 14 also recites selectively inserting compliant data into the second data stream after the PES header, to hold key information associated with the PES header. Since *Gray* does not describe copying a first data stream to create a second data stream, it also does not describe inserting compliant data into the second data stream. Reviewing the portions of *Gray* that the Office cited in rejecting claim 1, none of those portions describes the above limitation. Nor does any other portion of *Gray* describe the above limitation. Therefore, *Gray* fails to teach at least this limitation of claim 14 and does not anticipate claim 14.

Regarding that portion of claim 14 reciting the insertion of key information, Applicants rely on their argument in support of claim 8 that key information is non-compliant data and that *Gray* does not describe a KSB as key information. Applicants also rely on their arguments in regard to claim 1 that *Gray* does not describe a KSB as non-compliant data. Applicants also note their argument in support of claim 4 that the KSB is not used in performing encryption and decryption.

For at least the above reasons, claim 14 is separately patentable and it is requested that the Board overturn the rejection of claim 14.

14. Regarding Claim 15

Dependent claim 15 modifies the machine-accessible medium of claim 14 to recite, “storing the first data stream; and storing the second data stream.” In rejecting claim 15, the

Office cites col. 4, lines 47-67 of *Gray*. (Office Action, p. 6, ¶ 23). This portion of *Gray* describes defining a bit in a header as a KSB and describes use of the KSB as a signal to a destination node to activate a new key. But the cited passage does not describe storing first and second data streams. Applicants could not find any other portion of *Gray* that describes the above limitation.

For at least the above reasons, claim 15 is separately patentable and it is requested that the Board overturn the rejection of claim 15.

15. Regarding Claim 16

Dependent claim 16 modifies the machine-accessible medium of claim 14 to recite, “parsing the second data stream to find each PES header; embedding key information into each portion of the second data stream after each PES header; and encrypting each portion of the second data stream.” In rejecting claim 16, the Office cites col. 4, lines 47-67 of *Gray*. (Office Action, p. 6, ¶ 23). This portion of *Gray* describes defining a bit in a header as a KSB and describes use of the KSB as a signal to a destination node to activate a new key. But the cited passage does not describe any operations with a second data stream. It is unclear why the Office cited the above passage as relevant to claim 16. Regardless, the cited passage does not describe the limitations of claim 16. Applicants could not find any other portion of *Gray* that describes any of the above limitations of claim 16.

For at least the above reasons, claim 16 is separately patentable and it is requested that the Board overturn the rejection of claim 16.

16. Regarding Claim 17

Dependent claim 17 modifies the machine-accessible medium of claim 14 to recite, “transmitting each portion of the second data stream.” In rejecting claim 17, the Office cites col.

5, lines 17-35 of *Gray*. (Office Action, p. 7, ¶ 24). As discussed above regarding claim 16, this portion of *Gray* describes the source node changing the KSB bit value when a new key is activated. It also describes a destination node activating a new key in response to the changed KSB value. But the cited passage does not describe any operations with a second data stream and certainly does not describe transmitting a second data stream. It is unclear why the Office cited the above passage as relevant to claim 17. Regardless, the cited passage does not describe the limitations of claim 17. Applicants could not find any other portion of *Gray* that describes any of the above limitation of claim 17.

For at least the above reasons, claim 17 is separately patentable and it is requested that the Board overturn the rejection of claim 17.

17. Regarding Claim 18

Dependent claim 18 modifies the machine-accessible medium of claim 16 so that the method further comprises: “retrieving key information from a portion of the second data stream; decrypting the portion of the second data stream with the key information; and replacing the key information with compliant data in the portion of the second data stream.”

In rejecting claim 18, the Office cites col. 5, lines 17-35 of *Gray*. (Office Action, p. 7, ¶ 24). As discussed above, this portion of *Gray* describes the source node changing the KSB bit value when a new key is activated. It also describes a destination node activating a new key in response to the changed KSB value. But the cited passage does not describe any operations with a second data stream and certainly does not describe the retrieving, decrypting, and replacing operations of claim 18. It is unclear why the Office even cited the above passage as relevant to claim 18. Applicants could not find any other portion of *Gray* that describes any of the above limitations of claim 18.

For at least the above reasons, claim 18 is separately patentable and it is requested that the Board overturn the rejection of claim 18.

18. Regarding Claim 19

Dependent claim 19 modifies the machine-accessible medium of claim 16 so that the method further comprises “decoding the portion.” In rejecting claim 19, the Office cites col. 5, lines 17-35 of *Gray*. (Office Action, p. 7, ¶ 24). As discussed above, this portion of *Gray* describes the source node changing the KSB bit value when a new key is activated. It also describes a destination node activating a new key in response to the changed KSB value. But the cited passage does not describe any operations with a second data stream and certainly does not describe decoding a portion of the second data stream, as recited in claim 19. Again, it is unclear why the Office even cited the above passage as relevant to claim 19. Regardless, the cited passage does not describe the limitations of claim 19. Applicants could not find any other portion of *Gray* that describes any of the above limitation of claim 19.

Applicants also rely on their argument in support of claim 1 that *Gray* does not describe decodable data streams or decoding.

For at least the above reasons, claim 19 is separately patentable and it is requested that the Board overturn the rejection of claim 19.

C. Claims Rejected Under 35 U.S.C. § 103(a)

The Examiner rejected claims 20-25 under 35 U.S.C. § 103(a) as unpatentable over *Gray*. For at least the reasons discussed below, claims 20-25 are not rendered obvious by *Gray*.

1. Regarding Claims 20, 24, 25

Independent claim 20 provides:

20. (Previously Presented) A method, comprising:

transmitting a data structure to a consumption device, the data structure including a header,
key information separate from and associated with the header for use in decryption, and
a payload associated with the header, **the payload capable of being encrypted using the key information.**
(Emphasis added).

To establish a *prima facie* case of obviousness, the Office must show that the cited reference teaches or suggests each of the elements of the claim. This includes the first emphasized element of “key information separate from and associated with the header.” The Applicants believe that *Gray* fails to teach the elements of claims 20 and 25, because the key synchronization bit of *Gray* is found within the header. See *Gray*, col. 4, lines 49-52. The Office has argued that this difference is merely the “rearranging of parts.” However, the rearrangement of parts in *In re Japiske*, 181 F.3d 1019, 86 U.S.P.Q. 70 (CCPA, 1950), did not affect the operation of the device. Moving data outside of a header affects the operation of *Gray*. *Gray*, as is common in the art, only analyzes the header. Analyzing the remainder of the packet to determine an additional data structure that is neither payload nor header would alter a fundamental operating principle of *Gray*. See MPEP § 2143.01 (IV). Thus, *Gray* cannot be modified as suggested by the Office.

The second emphasized portion of claim 20 recites, “the payload capable of being encrypted using the key information.” *Gray* does not describe the data being encrypted using the KSB. Instead, *Gray* consistently refers to the KSB as being read by the destination node, which performs decryption. (See, e.g., *Gray*, col. 2, lines 65-67). This is another element not taught or suggested by *Gray*.

The Office cites the “Data Field” of Fig. 5, as teaching the above payload element that is capable of being encrypted using the key information. (Office Action, p. 7, ¶ 27). But the Office does not cite any part of *Gray* describing the “Data Field” as “capable of being encrypted using” the KSB that the Office regards as the “key information.”

Applicants also rely on their arguments in support of claims 8 that key information is non-compliant data and in support of claim 1 and 8 that the KSB is not described by *Gray* as non-compliant data.

For at least the above reasons, independent claims 20 and 25 are separately patentable and it is requested that the Board overturn the rejection of claims 20 and 25. Claim 24 depends from patentable claim 20 and it is therefore requested that the Board overturn the rejection of claim 24.

2. Regarding Claim 21

Dependent claim 21 modifies the method of claim 20 by reciting that, “compliant data replaces the key information associated with the header, before decryption.” Claim 20 recites that the payload data is capable of being encrypted using the key information. So claim 21 recites replacing key information that can be used for encryption, with compliant data. In regard to other claims, the Office has argued that flipping the bit value of the KSB constitutes replacing non-compliant data with compliant data. (See, e.g., Advisory Action, Continuation Sheet – “Examiner would point out that Gray teaches replacing/changing the KSB value to a 1 or 0” However, the Office cannot show that either the 1 or the 0 bit value of the KSB is key information can be used for encryption. Since the KSB is not described as key information useful for encryption, changing its value prior to decryption does not meet the above limitation of claim 21 of replacing non-compliant data with compliant data prior to decryption.

In rejecting claim 21, the Office cites col. 5, lines 23-34 of *Gray* as describing “replacing the non-compliant data near the synchronization point with compliant data, and decoding the portion of the data stream.” (Office Action, p. 8, ¶ 28). This portion of *Gray* describes a method of using the KSB bit value as a signal to a destination node to activate and use a new key for decryption. But, there is nothing in the cited passage that describes replacing key information (even if one assumes *arguendo* that the KSB is key information) that can be used in encryption.

For at least the above reasons, claim 21 is separately patentable and it is requested that the Board overturn the rejection of claim 21.

3. Regarding Claim 22

Dependent claim 22 modifies the method of claim 21 to recite that “the header, compliant data, and decrypted payload are capable of being decoded by a compliant decoder.” In rejecting claim 22, the Office cites col. 5, lines 23-34 of *Gray* as describing “replacing the non-compliant data near the synchronization point with compliant data, and decoding the portion of the data stream.” (Office Action, p. 8, ¶ 28). But the Office again incorrectly equates decrypting and decoding. Claim 21 recites decrypting. Claim 22 recites decoding. Under claim differentiation, the two are different. Applicants rely on their argument in support of claim 1 that *Gray* does not describe a decodable data stream or decoding. There is nothing in the cited portion of *Gray*, or any other portion of *Gray*, describing decoding.

For at least the above reasons, claim 22 is separately patentable and it is requested that the Board overturn the rejection of claim 22.

4. Regarding Claim 23

Dependent claim 23 modifies the method of claim 20 to recite that “the key information in the header replaces compliant data, after encryption.” Applicants rely on their argument in

support of claim 8 that key information is non-compliant data. Thus, claim 20 recites replacing compliant data with non-compliant data. The Office has argued that changing the bit value of the KSB is the same as replacing non-compliant data with compliant data. But the Office cannot have it both ways. The changed bit value cannot be both non-compliant and compliant data.

Applicants also rely on their previous argument in support of claim 8 that the KSB does not correspond to the claimed key information.

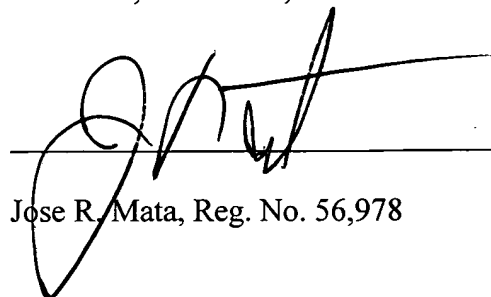
In rejecting claim 23, the Office cites col. 5, lines 17-35 of *Gray*. But the cited passage is cited as describing something other than the above limitation of claim 23. It is unclear why this passage is cited by the Office as relevant to claim 23.

For at least the above reasons, claim 23 is separately patentable and it is requested that the Board overturn the rejection of claim 23.

Based on the foregoing, the Board should overturn the rejection of all pending claims and hold that all of the claims currently pending in the application under review are allowable.

Dated: October 18, 2006 Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP



Jose R. Mata, Reg. No. 56,978

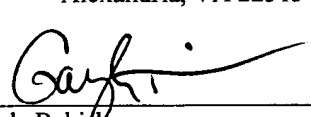
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025

(310) 207-3800

CERTIFICATE OF MAILING

I hereby certify that the correspondence is being deposited with the United States Postal Service as first class mail in an envelope with adequate postage affixed, addressed to:

Assistant Commissioner for Patents
Board of Patent Appeals and Interferences
P.O. Box 1450
Alexandria, VA 22313-1450



Gayle Bekish

10/18/06
Date

VIII. CLAIMS APPENDIX

The claims involved in this appeal are presented below.

1. (Original) A method, comprising:

parsing a data stream to find a predefined synchronization point within the data stream;

and

placing non-compliant data near the synchronization point in the data stream;

wherein the data stream is decodable by a compliant decoder, after the non-compliant data is replaced with compliant data.

2. (Original) The method as recited in claim 1, further comprising:

encrypting a portion of the data stream; and

transmitting the portion of the data stream.

3. (Original) The method as recited in claim 2, further comprising:

decrypting the portion of the data stream.

4. (Original) The method as recited in claim 3, wherein the non-compliant data is key information that is used in encrypting and decrypting.

5. (Previously Presented) A method, comprising:

receiving a portion of a data stream;

parsing the portion of the data stream to find a synchronization point within the data stream;

retrieving non-compliant data near the synchronization point;
replacing non-compliant data in the data stream; and
decrypting the portion of the data stream.

6. (Original) The method as recited in claim 5, wherein the non-compliant data is key information that is used in decrypting.

7. (Original) The method as recited in claim 5, further comprising:
replacing the non-compliant data near the synchronization point with compliant data; and
decoding the portion of the data stream.

8. (Previously Presented) A system, comprising:
an authoring device to use key information to encrypt a portion of a data stream; and
a consumption device in communication with the authoring device, the consumption device to use the key information to decrypt the portion of the data stream and to replace the key information with compliant data.

9. (Original) The system as recited in claim 8, further comprising:
a decoding device in communication with the consumption device to decode the portion of the data stream.

10. (Original) The system as recited in claim 8, wherein the consumption device is configured to retrieve the key information from the portion of the data stream.

11. (Original) A system, comprising:
an authoring device to create a data stream;
an encryption tool to embed key information near each synchronization point in the data stream and to encrypt a portion of the data stream associated with each synchronization point;
and
a consumption device to retrieve key information near each synchronization point in the data stream and to replace the key information with compliant data and to use the key information to decrypt the data stream.

12. (Original) The system as recited in claim 11, further comprising:
a decoding device to decode the data stream.

13. (Original) The system as recited in claim 11, further comprising:
a decryption tool to use the key information to decrypt the portion.

14. (Original) A machine-accessible medium having associated content capable of directing the machine to perform a method, the method comprising:
parsing a first data stream to find a packetized elementary stream (PES) header, the PES header associated with at least some payload data;
copying the first data stream to a second data stream; and
selectively inserting compliant data into the second data stream after the PES header, to hold key information associated with the PES header.

15. (Original) The machine-accessible medium as recited in claim 14, wherein the method further comprises:

storing the first data stream; and
storing the second data stream.

16. (Original) The machine-accessible medium as recited in claim 14, wherein the method further comprises:

parsing the second data stream to find each PES header;
embedding key information into each portion of the second data stream after each PES header; and
encrypting each portion of the second data stream.

17. (Original) The machine-accessible medium as recited in claim 16, wherein the method further comprises:

transmitting each portion of the second data stream.

18. (Original) The machine-accessible medium as recited in claim 16, wherein the method further comprises:

retrieving key information from a portion of the second data stream;
decrypting the portion of the second data stream with the key information; and
replacing the key information with compliant data in the portion of the second data stream.

19. (Original) The machine-accessible medium as recited in claim 18, wherein the method further comprises:

decoding the portion.

20. (Previously Presented) A method, comprising:

transmitting a data structure to a consumption device, the data structure including a header,

key information separate from and associated with the header for use in decryption, and

a payload associated with the header, the payload capable of being encrypted using the key information.

21. (Previously Presented) The method of claim 20, wherein compliant data replaces the key information associated with the header, before decryption.

22. (Previously Presented) The method of claim 21, wherein the header, compliant data, and decrypted payload are capable of being decoded by a compliant decoder.

23. (Previously Presented) The method of claim 20, wherein the key information in the header replaces compliant data, after encryption.

24. (Previously Presented) The method of claim 20, wherein the header is a packetized elementary stream (PES) header and the payload is a PES payload.

25. (Previously Presented) A machine-readable medium, having a set of instructions stored thereon, which when executed cause a machine to perform a set of operations comprising;

transmitting a data structure to a consumption device, the data structure including:

a header,

key information separate from and associated with the header for use in decryption, and

a payload associated with the header, the payload capable of being encrypted using the key information.

IX. EVIDENCE APPENDIX

No evidence is submitted with this appeal.

X. RELATED PROCEEDINGS APPENDIX

No related proceedings exist.